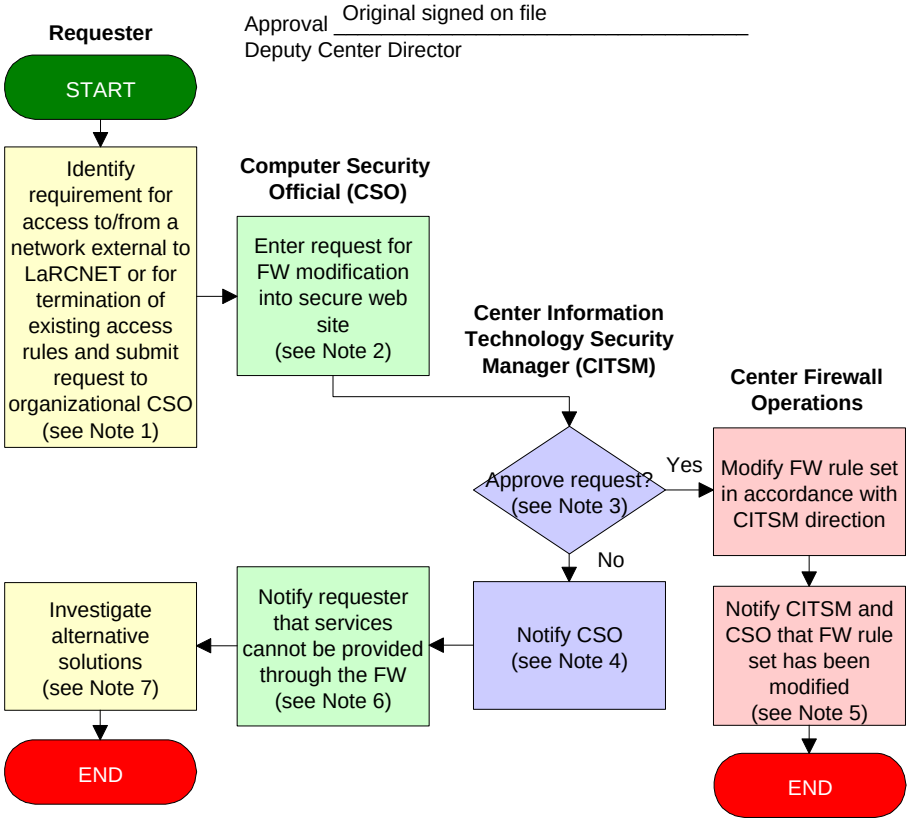
ACCESSING NETWORK SERVICES THROUGH THE CENTER FIREWALL

LMS-CP-5696
Revision: D-3

Objectives:
-to track changes to the rule set for the Langley center firewall (FW)
-to ensure that network services that traverse the FW, in either direction, do not pose an unacceptable level of risk to the Langley network (LaRCNET)

Approval Original signed on file
Deputy Center Director



General Information

The following records are generated by this procedure and are maintained in accordance with CID 1440.7:
-Modification to Firewall Rules

ACRONYMS

CIO	Chief Information Officer
CITSM	Center IT Security Manager
CSO	Computer Security Official
FW	Firewall
IP	Internet Protocol
IT	Information Technology
LaRCNET	Langley network
NPR	NASA Procedural Requirements
PKI	Public Key Infrastructure

Note 1
A list of organizational CSO's can be accessed at the following web site:
http://itsecurity.larc.nasa.gov/

All communications with the CSO must be either verbal; in writing; or via PKI encrypted e-mail. The CSO must be given detailed information about the services requested through the FW including, but not limited to (1) source and destination IP addresses; (2) source and destination ports; and (3) duration of requirement.

The CSO may decide to deny the request, without submitting a formal request for a modification to the FW rule set.

Note 2
This procedure requires CSO's to possess a PKI certificate (see LMS-CP-5630) to send and receive encrypted e-mail, as well as a two-factor authentication token to access the secure web site (see LMS-CP-5915).

The CSO may initiate contact with the CITSM via PKI encrypted e-mail to clarify the IT security implications of the request.

The CSO logs into the secure web site (https://rugby.larc.nasa.gov) using two-factor authentication to initiate the change request. The web site maintains a record of requests for modifications to the FW, as well as the disposition. This action by the CSO initiates a clear-text e-mail to firewall@larc.nasa.gov to notify the CITSM and the FW team of a pending request. The CSO can view the status of FW rules or requested modifications at any time on the secure web site.

Note 3
The CITSM or his designee evaluates the threat based on criteria in NPR 2810.1, current intelligence data, and any agency or national alerts. If the service is appropriate, the CITSM approves the request on the secure web site, which initiates a clear-text message to firewall@larc.nasa.gov stating that a modification to the FW has been approved.

This e-mail directs that a scan be conducted on any Langley computer that will provide a service to external computers. Any vulnerabilities discovered must be corrected before the service can be provided through the FW. On a continuing basis, Langley computers that are accessible through the FW are scanned for vulnerabilities. If new vulnerabilities are discovered or old vulnerabilities reappear, the access through the FW may be terminated immediately if the threat is too great, or the CSO may be given some brief period of time to ensure the vulnerability is corrected if the threat does not appear to be imminent.

The evaluation of threats and vulnerabilities is dynamic. Under emergency conditions when NASA resources are being attacked or threatened a pre-emptive interruption of services may become necessary. The CITSM or center CIO or their designees may give verbal instruction to the center FW operations for immediate changes to the FW rule set to protect the integrity of LaRCNET.

Note 4
The CITSM sends PKI encrypted e-mail to the CSO explaining the reasons that the service cannot be provided, with a copy to the Langley CIO.

Note 5
The FW team completes the rule modification and initiates a clear-text message to firewall@larc.nasa.gov and the CSO stating that the requested FW modification has been completed.

Note 6
The CSO notifies the requester either verbally, in writing, or via PKI encrypted e-mail that the service cannot be provided through the firewall.

Note 7
The requester may consult with the CSO, CITSM or Langley IT security staff for alternative solutions to the requirement. This consultation should be either verbally, in writing, or via PKI encrypted e-mail.